SIRI & GLIMSTAD LLP
Kyle McLean (SBN 330580)
E: kmclean@sirillp.com
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 376-3739
Fax: (646) 417-5967

Mason Barney (*Pro Hac Vice to be filed*)
Email: mbarney@sirillp.com
Steven D. Cohen (*Pro Hac Vice to be filed*)
Email: scohen@sirillp.com
745 Fifth Ave, Suite 500
New York, NY 10151
Telephone: 212-532-1091
Facsimile: 646-417-5967

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ASHLEY PILLARD and DESTINY RUCKER, on behalf of themselves and all others similarly situated, Plaintiffs, v. PAYPAL, INC., Defendant.	Case No. 23-936 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Ashley Pillard and Destiny Rucker, individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiffs"), allege the following against PayPal, Inc. ("PayPal" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against PayPal for its failure to properly secure and safeguard Plaintiffs' and other similarly situated PayPal customers' names, addresses, Social Security numbers, individual tax identification numbers, dates of birth, or other sensitive records from hackers.

2. PayPal, based in San Jose, California, is an online payment platform that serves more than 400 million customers.

3. On or about January 18, 2023, PayPal filed official notice of a hacking incident with the Office of the Maine Attorney General. Under state law, organizations must report breaches involving personal information, including Social Security number, driver's license or state ID number, account number or credit or debit card number, account passwords, among other things.

4. Also, on or about January 18, 2023, PayPal sent out data breach letters to individuals whose information was compromised as a result of the recent data security incident.

5. Based on the Notice filed by the company, on December 20, 2022, PayPal detected unusual activity on some of its computer systems. In response, the company conducted an investigation. PayPal's investigation revealed that an unauthorized party had access to certain company files between December 6, 2022 and December 8, 2022 (the "Data Breach").

6. Plaintiffs and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes names, addresses, Social Security numbers, individual tax identification numbers, and/or dates of birth (collectively the "Private Information") and additional personally identifiable information ("PII") that PayPal collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, and a headstart, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names

to obtain medical services, using Class Members' information to obtain government benefits, and filing fraudulent tax returns using Class Members' information.

9. Therefore, Plaintiffs and Class Members have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

10. Plaintiffs bring this class action lawsuit to address PayPal's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

11. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to PayPal, and thus PayPal was on notice that failing to take necessary steps to secure the Private Information left that Private Information vulnerable to an attack.

12. PayPal and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had PayPal properly monitored its networks, it would have discovered the breach sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of PayPal's negligent conduct as the Private Information that PayPal collected and maintained is now likely in the hands of data thieves and unauthorized third-parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to PayPal's data security systems, future annual audits, and adequate credit monitoring services funded by PayPal.

PARTIES

16. Plaintiff Ashley Pillard is, and at all times mentioned herein was, an individual citizen of the State of Nebraska residing in the City of Lincoln.

17. Plaintiff Destiny Rucker is, and at all times mentioned herein was, an individual citizen of the State of Texas residing in the City of Garland.

18. Defendant PayPal is an online payment platform incorporated in Delaware with its headquarters in San Jose, California.

JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from PayPal. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over the Defendant because it operates in and is headquartered in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Upon information and belief, PayPal has harmed Class Members residing in this District.

DIVISIONAL ASSIGNMENT

22. PayPal has its headquarters in San Jose, California and thus assignment to the San Jose division is appropriate here.

PAYPAL COLLECTS HIGHLY SENSITIVE CUSTOMER INFORMATION

23. PayPal is an online payment platform. Founded in 1998, PayPal is the world's most widely used payment acquirer, serving more than 400 million customers. PayPal employs more than 30,000 people and generates more than $25 billion in annual revenue.

24. As a condition of providing online payment services, PayPal requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from PayPal, some customers are required to provide sensitive personal and private information such as:

- Names;

- Addresses;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers and information;
- Individual tax identifical numbers;
- Financial account information; and
- Payment card information.

25. PayPal uses this information, *inter alia*, to verify customers' identities and to process payments.

26. In its privacy policy, PayPal promises its customers that "keep[ing] [] personal information safe against loss, misuse, unauthorized access, disclosure, and alteration is our top priority."[1]

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, PayPal assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

28. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

29. Plaintiffs and Class Members relied on PayPal to keep their Private Information confidential and securely maintained and to make only authorized disclosures of this information.

PAYPAL'S DATA BREACH AND NOTICE TO PLAINTIFFS

30. Plaintiffs were customers of PayPal. As part of Plaintiffs utilizing PayPal as their online payment processor, PayPal collected, *inter alia*, names, addresses, Social Security numbers, individual tax identification numbers, and dates of birth for Plaintiffs.

[1] *See* PayPal Privacy Statement, https://www.paypal.com/us/legalhub/privacy-full?locale.x=en_US#:~:text=We%20do%20not%20sell%20your,to%20manage%20our%20Rewards%20program (last visited Mar. 2, 2023).

31. According to the company, on December 20, 2022, PayPal learned of unauthorized access to its computer systems, which the company eventually determined occurred between December 6 and December 8, 2022. The unauthorized individual or individuals accessed a cache of highly sensitive PII, including names, addresses, Social Security numbers, individual tax identification numbers, and dates of birth.

32. According to media reports, the unauthorized individual or indivdiuals used a "credential stuffing" cyberattack to access the accounts in question. In a credential stuffing attack, the hacker aquires usernames and passwords or password hash codes that were exposed in prior breaches, either of the targeted company or of a third party company, and then repeatedly enters those combinations until the hacker gains access to an account. Shuman Ghosemajumder, an executive at Google, estimated in 2017 that credential stuffing has a roughly 2% success rate, meaning that if a hacker tried 1 million username and password combinations, approximately 20,000 would be successful.[2]

33. On or about January 18, 2023, PayPal began to notify customers that its investigation identified that their Personal Information was breached. The Data Breach Notification Letters alerted Plaintiffs and Class Members that their highly sensitive PII had been exposed in "an incident."

34. The Data Breach Notification Letter to Plaintiffs stated: "The personal information that was exposed could have included your name, address, Social Security number, individual tax identification number, and/or dale of birth." Thus, the company left it unclear exactly what pieces of Plaintiffs' Personal Information was stolen.

35. The Data Breach Notification Letter then attached several pages entitled "Additional Resources," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing an online link that victims could click on if they "have any

[2] Ghosemajumder, Shuman, "You Can't Secure 100% of Your Data 100% of the Time". *Harvard Business Review* (2017) *available at* https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time (last visited Mar. 2, 2023).

questions," PayPal offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves.

36. On information and belief, PayPal sent a similar generic letter to all individuals affected by the Data Breach.

37. PayPal had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

38. Plaintiffs and Class Members provided their Private Information to PayPal with the reasonable expectation and mutual understanding that PayPal would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

39. PayPal's data security obligations were particularly important given the substantial increase in cyberattacks. According to industry sources, simple and common precautions like using two-factor authentication or requiring stronger password requirements will foil most credential stuffing attacks. On information and belief, PayPal failed to require such precautions for all users.

40. PayPal knew or should have known that its electronic records would be targeted by cybercriminals.

PAYPAL FAILED TO COMPLY WITH FTC GUIDELINES

41. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decisionmaking.

42. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any

security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

43. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

45. Credential Stuffing was such a concern for companies that six years ago in 2017, the FTC issued specific guidance regarding how to avoid such attacks. Among other things, the FTC stated that to combat such attacks, "companies should combine multiple authentication techniques for accounts with access to sensitive data."[3]

46. On information and belief, PayPal failed to properly implement basic data security practices. PayPal's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

47. PayPal was at all times fully aware of the FTC guidelines and its obligation to protect the PII of its customers.

---

[3] *"Stick with Security: Require secure passwords and authentication"*. Federal Trade Commission. (2017), *available at* https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-require-secure-passwords-and-authentication (last visited Mar. 2, 2023)

PAYPAL FAILED TO COMPLY WITH INDUSTRY STANDARDS

48. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

49. Some industry best practices that should be implemented by businesses like PayPal include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. Upon information and belief, Defendant failed to follow some or all of these industry best practices.

50. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding these points. Upon information and belief, Defendant failed to follow these cybersecurity best practices, including failure to train its staff.

51. Upon information and belief, Defendant failed to meet the minimum standards of any of the following frameworks, thereby opening the door to the cyber incident and causing the Data Breach: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

PAYPAL'S SECURITY OBLIGATIONS

52. PayPal breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data. PayPal's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of PII;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of Section 5 of the FTCA; and

f. Failing to adhere to industry standards for cybersecurity.

53. PayPal negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

54. Accordingly, as outlined below, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with PayPal.

DATA BREACHES, FRAUD, AND IDENTITY THEFT

55. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[4] Exposure of personal information that a consumer wishes to keep private may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

[4] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf. (last visited Mar. 2, 2023).

56. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

57. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[5]

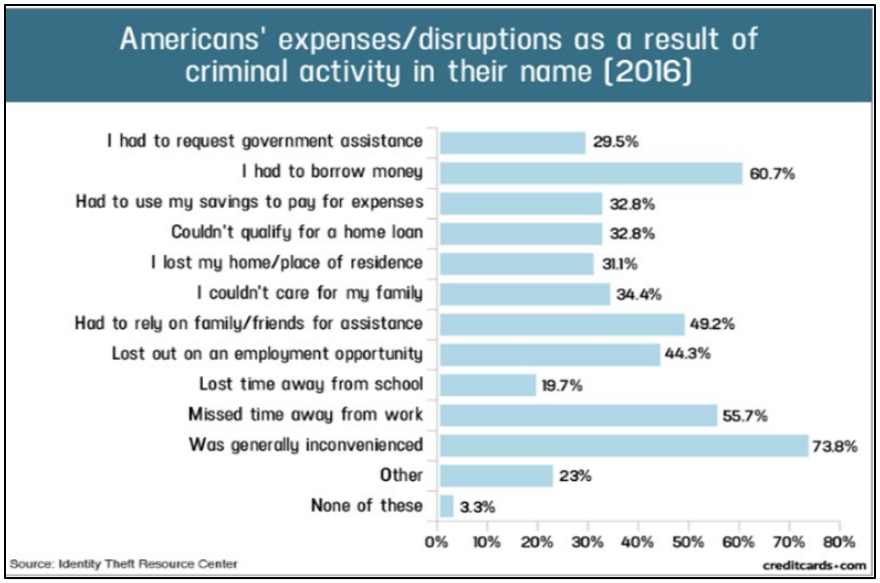
58. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

59. Identity thieves can also use Social Security numbers to obtain official identification card in the victim's name but with the thief's picture, use the victim's name and Social Security number to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social

[5] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Mar. 2, 2023).

Security number, rent a house or receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

60. A study by the Identity Theft Resource Center[6] shows the multitude of harms caused by fraudulent use of PII:



61. Moreover, the value of Private Information is axiomatic. The value of "big data" in corporate America is astronomical. Meanwhile, the consequences of cyberthefts include heavy prison sentences. The fact that identity thieves attempt to steal identities notwithstanding these possible heavy prison sentences illustrates beyond a doubt that Private Information has considerable market value.

62. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[7]

---

[6] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Mar. 2, 2023).

[7] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Mar. 2, 2023).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

63. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

64. As a result, there is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

65. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

66. Plaintiffs' Private Information, including sensitive PII, was compromised as a direct and proximate result of the Data Breach.

67. As a direct and proximate result of PayPal's conduct, Plaintiffs and Class Members have suffered an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

68. As a direct and proximate result of PayPal's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

69. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as medical services billed in their names, loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

70. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information, as potential

fraudsters could use that information to target their schemes more effectively to Plaintiffs and Class Members.

71. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

72. The information that PayPal maintains regarding Plaintiffs and Class Members combined with publicly available information allows nefarious actors to assemble a detailed picture of Plaintiffs' and Class Members' history.

73. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to PayPal was intended to be used by PayPal to fund adequate security of PayPal's computer property and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

74. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their accounts and records for misuse.

75. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

76. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of PayPal, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

77. As a direct and proximate result of PayPal's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and either have suffered harm or are at an increased risk of future harm.

CLASS ALLEGATIONS

78. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all other persons similarly situated (the "Class").

79. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a

notice of the Data Breach.

Nebraska Subclass

All residents of Nebraska who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Texas Subclass

All residents of Texas who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

80. Excluded from each of the above Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

81. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

82. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

83. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 34,942 customers of PayPal whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through PayPal's records, Class Members' records, publication notice, self-identification, and other means.

84. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether PayPal engaged in the conduct alleged herein;

b. Whether PayPal's conduct violated The Nebraska Consumer Protection Act, the Nebraska Uniform Deceptive Trade Acts, and the Texas Deceptive Trade Practices Act, invoked below;

c. When PayPal actually learned of the Data Breach and whether its response was adequate;

d. Whether PayPal unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether PayPal failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether PayPal's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether PayPal's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether PayPal owed a duty to Class Members to safeguard their Private Information;

i. Whether PayPal breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether PayPal had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether PayPal breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether PayPal knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of PayPal's misconduct;

o. Whether PayPal's conduct was negligent;

p. Whether PayPal's conduct was *per se* negligent;

q. Whether PayPal was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

85. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

86. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

87. Predominance. PayPal has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from PayPal's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

88. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PayPal.

In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

89. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). PayPal has acted or has refused to act on grounds generally applicable to the Class so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

90. Finally, all members of the proposed Class are readily ascertainable. PayPal has access to the names, addresses, and emails of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by PayPal.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NEBRASKA AND TEXAS STATE SUBCLASSES)

91. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

92. PayPal knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

93. PayPal's duty included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

94. PayPal knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and the Class Members and the importance of adequate security. PayPal was on notice because on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

95. PayPal owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. PayPal's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the Nebraska Consumer Protection Act, the Nebraska Uniform Deceptive Trade Practices Act, and the Texas Deceptive Trade Practices—Consumer Protection Act;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

96. PayPal's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because it was bound by industry standards to protect confidential Personal Information.

97. Plaintiffs and the Class Members were foreseeable victims of any inadequate security practices on the part of PayPal, and PayPal owed them a duty of care to not subject them to an unreasonable risk of harm.

98. PayPal, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within PayPal's possession.

99. PayPal, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

100. PayPal, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

101. PayPal breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information; and

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

102. PayPal had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust PayPal with their Private Information was predicated on the understanding that PayPal would take adequate security precautions. Moreover, only PayPal had the ability to protect its systems (and the Private Information that it stored on them) from attack.

103. PayPal's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

104. As a result of PayPal's failure to definitively notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

105. PayPal's breaches of duty caused a foreseeable risk to Plaintiffs and Class Members that they would be harmed by suffering from identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

106. As a result of PayPal's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

107. PayPal also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

108. As a direct and proximate result of PayPal's negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of further harm.

109. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

110. The injury and harm that Plaintiffs and Class Members suffered was the direct and proximate result of PayPal's negligent conduct.

111. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

112. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring PayPal to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NEBRASKA AND TEXAS STATE SUBCLASSES)

113. Plaintiffs restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

114. Pursuant to Section 5 of the FTCA, PayPal had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information, including PII, of Plaintiffs and Class Members.

115. PayPal breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to: proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

116. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

117. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information. The FTC publications described above and the industry-standard cybersecurity measures also form part of the basis of PayPal's duty in this regard.

118. PayPal violated the FTCA by failing to use reasonable measures to protect Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

119. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to PayPal's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' Personal Information.

120. PayPal's violations of the FTCA constitute negligence *per se*.

121. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to PayPal's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

122. As a direct and proximate result of PayPal's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information (including PII) because of the Data Breach, including but not limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

123. PayPal breached its duties to Plaintiffs and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

124. As a direct and proximate result of PayPal's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

125. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring PayPal to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NEBRASKA AND TEXAS STATE SUBCLASSES)

126. Plaintiffs restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

127. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to PayPal in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

128. PayPal's Privacy Policy memorialized the rights and obligations of PayPal and its customers. This document was provided to Plaintiffs and Class Members in a manner in which and during a time when it became part of the agreement for services.

129. In the Privacy Policy, PayPal commits to protecting the privacy and security of private information and promises to never share customer information except under specified circumstances with specific third-parties.

130. Plaintiffs and the Class Members fully performed their obligations under their contracts with PayPal.

131. However, PayPal did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' PII, and therefore PayPal breached its contract with Plaintiffs and Class Members.

132. PayPal allowed third-parties to access, copy, and/or transfer Plaintiffs' and Class Members' PII without permission. Therefore, PayPal breached the Privacy Policy with Plaintiffs and Class Members.

133. PayPal's failure to satisfy its confidentiality and privacy obligations resulted in PayPal providing services to Plaintiffs and Class Members that were of a diminished value.

134. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein.

135. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring PayPal to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NEBRASKA AND TEXAS STATE SUBCLASSES)

136. Plaintiffs restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

137. This Count is pleaded in the alternative to Count III above.

138. PayPal provides online payment processing services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for goods and services from Defendant.

139. Through Defendant's sale of goods and services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with PayPal's policies, practices, and applicable law.

140. As consideration, Plaintiffs and Class Members paid money to PayPal for online payment processing services, and turned over valuable PII to Defendant. Accordingly, Plaintiffs and Class Members bargained with PayPal to securely maintain and store their Personal Information.

141. PayPal violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Personal Information.

142. Plaintiffs and Class Members have been damaged by PayPal's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
VIOLATION OF THE NEBRASKA CONSUMER PROTECTION ACT
(ON BEHALF OF PLAINTIFF PILLARD AND THE NEBRASKA STATE SUBCLASS)

143. Plaintiff Pillard restates and realleges the allegations in paragraphs 1-90 as if fully set forth herein.

144. Plaintiff Pillard, members of the Nebraska state subclass, and PayPal each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Consumer Protection Act (the "CPA"), Neb. Rev. Stat. § 59-1601, *et seq*.

145. As fully alleged above, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Pillard's and members of the Nebraska state subclass' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Pillard's and members of the Nebraska state subclass' Private Information, including duties imposed by the FTCA, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that PayPal would protect the privacy and confidentiality of Plaintiff Pillard's and members of the Nebraska state subclass' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that PayPal did not reasonably or adequately secure Plaintiff Pillard's and members of the Nebraska state subclass' Private Information; and

g. Omitting, suppressing, and concealing the material fact that PayPal did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Pillard's and members of the Nebraska state subclass' Private Information.

146. PayPal's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PayPal's data security and ability to protect the confidentiality of consumers' Private Information.

147. PayPal knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff Pillard and members of the Nebraska state subclass, to deter hackers, and to detect a data breach within a reasonable amount of time. PayPal knew or should have known that the risk of a data breach was highly likely.

148. PayPal's conduct described above is a violation of the CPA, Neb. Rev. Stat. § 59-1603, as it is and was a restraint on trade or commerce. PayPal's violations have caused financial injury to Plaintiff Pillard and members of the Nebraska state subclass.

149. PayPal's violation of the CPA has an impact of great or general importance on the public.

150. As a direct and proximate result of PayPal's violation of the CPA, Plaintiff Pillard and members of the Nebraska state subclass are entitled to a judgment under Neb. Rev. Stat. § 59-1609 to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other further relief as the Court deems just and proper.

COUNT VI
VIOLATION OF THE NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT
(ON BEHALF OF PLAINTIFF PILLARD AND THE NEBRASKA STATE SUBCLASS)

151. Plaintiffs restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

152. Plaintiff Pillard, members of the Nebraska state subclass, and PayPal each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301, *et seq.*

153. PayPal's representations that it would adequately safeguard Plaintiff Pillard's and members of the Nebraska state subclass' Private Information constitute representations as to characteristics, uses, or benefits of services that such services did not actually have in violation of Neb. Rev. Stat. § 87-302(a)(5).

154. PayPal's representations that it would adequately safeguard Plaintiff Pillard's and members of the Nebraska state subclass' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as PayPal's data security services were of a lesser standard, quality, or grade) in violation of Neb. Rev. Stat. § 87-302(a)(8).

155. PayPal knowingly made false or misleading statements in its Privacy Policy regarding the use of personal information submitted by its customers, including that "[h]elping to keep [customers'] personal information against loss, misuse, unauthorized access, disclosure, and alteration is [PayPal's] top priority."[8]

156. PayPal did not securely maintain personal information as it had represented, in violation of Neb. Rev. Stat. § 87-302(a)(15).

157. The above UDTPA violations have caused financial injury to Plaintiff Pillard and members of the Nebraska state subclass and have created an imminent risk of future injury.

158. Accordingly, Plaintiff Pillard, on behalf of herself and the members of the Nebraska state subclass, bring this claim under the UDTPA to seek such injunctive relief as is necessary in order to enjoin further violations and to recover the costs of this action, including reasonable attorneys' fees and costs.

COUNT VII
TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT
(ON BEHALF OF PLAINTIFF RUCKER AND THE TEXAS STATE SUBCLASS)

159. Plaintiff Rucker and members of the Texas state subclass restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

160. PayPal, Plaintiff Rucker, and members of the Texas state subclass are persons as defined by Tex. Bus. & Com. Code § 17.45(3).

161. Plaintiff Rucker and members of the Texas state subclass are consumers as defined by Tex. Bus. & Com. Code § 17.45(4).

[8] *See* PayPal Privacy Statement, https://www.paypal.com/us/legalhub/privacy-full?locale.x=en_US#:~:text=We%20do%20not%20sell%20your,to%20manage%20our%20Rewards%20program (last visited Mar. 2, 2023).

162. PayPal advertised, offered, or sold services in Texas and engaged in trade or commerce, as defined by Tex. Bus. & Com. Code § 17.45(6), which directly or indirectly affected the people of Texas.

163. PayPal engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that its services have sponsorship, approval, characteristics, uses, benefits or quantities that they do not have;

b. Representing that its services are of a particular standard, quality, or grade when they are of a lesser standard, quality, or grade; and/or

c. Advertising services with the intent to not provide them as advertised.

164. PayPal's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Rucker and members of the Texas state subclass' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rucker's and members of the Texas state subclass' Private Information, including duties imposed by the FTCA and the Texas data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Rucker and members of the Texas state subclass' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rucker and members of the Texas state subclass' Private Information, including duties imposed by the FTCA and Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Rucker's and members of the Texas state subclass' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rucker's and members of the Texas state subclass' Personal Information, including duties imposed by the FTCA and Tex. Bus. & Com. Code § 521.052.

165. Upon information and belief, PayPal intended to mislead Plaintiff Rucker and members of the Texas state subclass and induce them to rely on its misrepresentations and omissions.

166. PayPal's representations and omissions were material because they were likely to deceive reasonable customers about the adequacy of its data security and its ability to protect the confidentiality of customers' Personal Information.

167. Had PayPal disclosed to Plaintiff Rucker and members of the Texas state subclass that its data systems were not secure and vulnerable to attack, PayPal would have been forced to adopt reasonable security measures and comply with the law in order to continue its business. Instead, PayPal represented that its data security was effective and it was trusted with sensitive

and valuable Personal Information regarding millions of customers, including Plaintiff Rucker and members of the Texas state subclass. PayPal accepted the responsibility of being a data steward while keeping the inadequate state of its security controls secret from the public. Accordingly, because PayPal held itself out as secure with a corresponding duty of trustworthiness and care, Plaintiff Rucker and members of the Texas state subclass acted reasonably in relying on PayPal's misrepresentations and omissions, the truth of which they could not have discovered.

168. PayPal engaged in unconscionable actions or courses of conduct in violation of Tex. Bus. & Com. Code § 17.50(a)(3). Specifically, PayPal engaged in acts or practices which took advantage of customers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

169. Consumers like Plaintiff Rucker and members of the Texas state subclass lacked knowledge of the deficiencies in PayPal's data security because this information was known exclusively by PayPal. Consumers meanwhile lacked the ability, experience, capacity, or expertise to secure or protect their interests in the Personal Information in PayPal's possession, custody, or control. Consumers like Plaintiff Rucker and members of the Texas state subclass also lacked sufficient expertise in data security measures and did not have access to PayPal's systems such that they could evaluate its security controls. PayPal took advantage of its access to customers' Personal Information in order to hide its inability to protect the security and confidentiality of Plaintiff Rucker's and members of the Texas state subclass' Personal Information.

170. On information and belief, PayPal intended to take advantage of consumers' lack of knowledge, ability, experience, capacity, and expertise to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from PayPal's conduct is glaring, flagrant, and unmitigated. The Data Breach resulting from PayPal's unconscionable business acts and practices exposed Plaintiff Rucker and members of the Texas state subclass to a wholly unwarranted risk to the safety of their Personal Information and the security of their identity or credit and also caused a substantial hardship for a significant number of PayPal customers.

171. Upon information and belief, PayPal acted intentionally, knowingly, and maliciously to violate the Texas Deceptive Trade Practices—Consumer Protection Act. In doing so, it recklessly disregarded Plaintiff Rucker's and members of the Texas state subclass' rights.

172. As a direct and proximate cause of PayPal's unconscionable and deceptive acts or practices, Plaintiff Rucker and members of the Texas state subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased imminent risk of fraud and identity theft, and loss of value of their Personal Information. PayPal's unconscionable and deceptive acts or practices were a proximate cause of Plaintiff Rucker's and members of the Texas state subclass' injuries, ascertainable losses, economic damages, and non-economic damages.

173. PayPal's violations of the Texas Deceptive Trade Practices—Consumer Protection Act present a continuing risk to Plaintiff Rucker and members of the Texas state subclass as well as to the general public.

174. Plaintiff Rucker and members of the Texas state subclass seek all monetary and non-monetary relief allowed by law, including economic damages, court costs, reasonably and necessary attorneys' fees, injunctive relief, and any other relief which the court deems proper.

COUNT VIII
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NEBRASKA AND TEXAS STATE SUBCLASSES)

175. Plaintiffs restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

176. This count is pleaded in the alternative to Counts III and IV above.

177. Plaintiffs and Class Members conferred a benefit on PayPal by paying for products and services that should have included cybersecurity protection to protect their Personal Information which Plaintiffs and Class Members did not adequately receive.

178. PayPal has retained the benefits of its unlawful conduct including the amounts received for cybersecurity practices that it did not provide. Due to PayPal's conduct alleged herein, it would be unjust and inequitable under the circumstances for PayPal to be permitted to retain the benefit of its wrongful conduct.

179. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from PayPal and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by PayPal from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

180. Plaintiffs and Class Members may not have an adequate remedy at law against PayPal, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IX
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NEBRASKA AND TEXAS STATE SUBCLASSES)

181. Plaintiffs restate and reallege the allegations in paragraphs 1-90 as if fully set forth herein.

182. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

183. PayPal owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Private Information.

184. PayPal possesses Private Information regarding Plaintiffs and Class Members.

185. Plaintiffs allege that PayPal's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private

Information and the risk remains that further compromises of their Private Information will occur in the future.

186. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. PayPal owes a legal duty to secure customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. PayPal's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. PayPal continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

187. This Court should also issue corresponding prospective injunctive relief requiring PayPal to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order PayPal to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that to comply with Defendant's explicit or implicit contractual obligations and duties of care, PayPal must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PayPal's systems on a periodic

basis, and ordering PayPal to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of PayPal's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps PayPal's customers must take to protect themselves.

188. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy to prevent another data breach at PayPal. The risk of another such breach is real, immediate, and substantial. If another breach at PayPal occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

189. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to PayPal if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other related damages. On the other hand, the cost of PayPal's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and PayPal has a preexisting legal obligation to employ such measures.

190. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at PayPal, thus preventing future injury to Plaintiffs and customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class and subclasses as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class and subclasses requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing PayPal to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring PayPal to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: March 2, 2023

Respectfully submitted,

/s/ Kyle McLean

SIRI & GLIMSTAD LLP
Kyle McLean (SBN 330580)
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 376-3739
E: kmclean@sirillp.com

Mason A. Barney (*pro hac vice* to be filed)
Steven D. Cohen (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: scohen@sirillp.com